Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Subject: COMPLAINT CLOSING
VOLPE Intrusion - C11N007CCU

Date: October 12, 2011

From: (b)(6), (b)(7)c
Computer Crimes Unit, JI-2

Reply to
Attn of: JI-2

To: File

On August 23, 2011, (b)(6), (b)(7)c Cyber Security Management Center (CSMC) advised the Computer Crimes Unit (CCU) of a recent compromise (b)(5), (b)(7)e According to (b)(5), (b)(6), (b)(7)c, (b)(7)e (b)(5), (b)(7)e CCU opened a complaint relating to this incident to determine if this activity was a result of intentional malicious activity conducted by a DOT employee or contractor or a targeted attack against certain individuals within VOLPE.

Based on a CSMC forensic report provided to CCU by (b)(6), (b)(7)c on September 9, 2011, the Initial Intrusion Vector (IIV) for this incident was a spear phishing email received by (b)(6), (b)(7)c VOLPE on August (b)(6), (b)(7)c 2011. (b)(6), (b)(7)c DOT system was infected with malware after clicking on a link contained within the spear phishing email. (b)(5), (b)(7)e (b)(5), (b)(6), (b)(7)c, (b)(7)e to CSMC, the spear phishing email and subsequent malicious activity was performed by overseas actors who used a known intrusion set to collect password hashes and perform off-line password cracking.

CSMC's report also identified vulnerabilities that made this compromise possible, including (but not limited to) the following:

[1] On Windows Server Systems, a **domain controller** (**DC**) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain.

(b)(5), (b)(7)e

Based upon a review of CSMC’s forensic report and subsequent conversation with

(b)(5), (b)(6), (b)(7)c, (b)(7)e

- # -

Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Subject: ACTION: Recommended Complaint Closing (b)(6), (b)(7)c - C12E004CCU

Date: October 3, 2012

From: (b)(6), (b)(7)c JI-2 CCU

Reply to Attn of: JI-2

To: (b)(6), (b)(7)c
Special Agent-in-Charge, JI-2

On July (b)(6), (b)(7)c 2012, this complaint was generated by an OIG project in order to determine if the unauthorized accesses of Department of Transportation (DOT) Information Technology (IT) resources were due to DOT employee misuse of computers, malicious insider activity, or poor cyber security practices. The DOT Office of Inspector General (OIG) conducted an in-depth review of DOT employee web activity in order to identify accesses to both high risk top level domains (i.e. foreign domains and websites) as well as websites identified as "most suspicious" by the SANS Internet Storm Center Website. The employee's web activity was matched with DOT's Cyber Security Management Center (CSMC) alerts data. (b)(6), (b)(7)c was identified as having potentially suspicious internet activity. In addition, there had been an unusually high number of CSMC alerts on computers in (b)(6), (b)(7)c work area.

OIG analysis of internet logs determined that (b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

OIG's forensics analysis of (b)(6), (b)(7)c DOT issued laptop did not identify any malicious activity. The analysis was able to confirm that (b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5)

Since OIG's preliminary inquiry and forensic analysis of (b)(6), (b)(7)c DOT issued computer did not identify any malicious activity, no further OIG investigative activity is anticipated. It is recommended that this complaint be closed.

- # -

Memorandum

U.S. Department of Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Subject: ACTION: OIG Investigation of (b)(6), (b)(7)c (C11N006CCU)

Date: October 17, 2011

From: William Swallow
Supervisory Special Agent
Computer Crimes Unit, JI-2

Reply to
Attn of: JI-2
(b)(6), (b)(7)c

To: Cheryl Ledbetter
Information Systems Security Officer (ISSO)
Federal Highway Administration (FHWA)

The memorandum summarizes the results of an Office of Inspector General (OIG) investigation involving (b)(6), (b)(7)c a GENEX systems (b)(6), (b)(7)c FHWA (b)(6), (b)(7)c and is being forwarded for your review and appropriate administrative action.

On August 1, 2011, the Cyber Security Management Center (CSMC) referred to the OIG Computer Crimes Unit (CCU) an incident (FY11-2925) that involved an unknown host and suspicious network traffic. The host was identified as a non-COE (Common Operating Environment) machine, but the IP addresses resolved back to FHWA. The (b)(5), (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

On September (b)(6), (b)(7)c 2011, (b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

[1] A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communications on the physical network segment.

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)5), (b)(6), (b)(7)c, (b)(7)e

This information is being referred back to FHWA for any administrative actions deemed appropriate. Please advise this office within 90 days of any action taken as a result of this memorandum.

If you have any questions, or if we can be of further assistance, please do not hesitate to contact (b)(6), (b)(7)c at (b)(6), (b)(7)c (b)(6), (b)(7)c.

##

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Memorandum

Subject: INFORMATION:
C11N004CCU : DOT SERVERS
(DOTHQNWMS005, OSTHQNWAS006)

Date: March 28, 2011

From: (b)(6), (b)(7)c
Computer Crimes Unit, JI-2

Reply to
Attn of: JI-2
(b)(6), (b)(7)c

To: File

On December (b)(6), (b)(7)c 2010, (b)(6), (b)(7)c US-CERT, contacted the DOT Cyber Security Management Center (CSMC) as well as the OIG's Computer Crimes Unit (CCU) about a computer security incident. (b)(6), (b)(7)c advised that US-CERT received information that two Internet Protocol (IP) (b)(5), (b)(7)e

(b)(5), (b)(7)e Any further information on this incident was classified.

On December (b)(6), (b)(7)c 2010, CCU spoke with (b)(6), (b)(7)c CSMC and (b)(5), (b)(7)c

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c, (b)(7)e

(b)(5), (b)(6), (b)(7)c

-----Original Message-----
From: (b)(6), (b)(7)c
Sent: Thursday, December 23, 2010 9:52 AM
To: Orndorff, Andrew (OST); (b)(6), (b)(7)c
(b)(6), (b)(7)c
Cc: (b)(6), (b)(7)c
Subject: Re: Update

I want to reiterate (b)(6), (b)(7)c word and want to personally thank all of your for your help. I look forward to working together more in the future.

In the mean time we will work with you to mitigate this current activity.

Sent using BlackBerry

On January (b)(6), (b)(7)c 2010, ORNDORFF advised that he spoke to (b)(6), (b)(7)c and received an unclassified update as to the status of the compromised servers:
STATUS:

(b)(5), (b)(6), (b)(7)c, (b)(7)e

4) US-CERT will provide USDOT a copy of the preliminary analysis report by COB 1/6/2011.

(b)(5), (b)(6), (b)(7)c

6) US-CERT has authorized USDOT to remediate the servers identified in the original incident/data request and to return them to full, production service.

CCU is closing this complaint due to the fact that US-CERT has obtained the data they requested, (b)(5), (b)(6), (b)(7)c (b)(5), (b)(6), (b)(7)c CCU support is no longer required.

- # -

Memorandum

U.S. Department of
Transportation

Office of the Secretary
of Transportation

Office of Inspector General

Subject: INFORMATION: Forensic Analysis of OIG Laptop (C11N001CCU)

Date: November 15, 2010

From: (b)(6), (b)(7)c
Computer Crimes Coordinator, JI-2

Reply to Attn of: JI-2
(b)(6), (b)(7)c

To: (b)(6), (b)(7)c
Acting, Chief Information Officer, JM-40

Attached for your information is a Forensic Media Analysis (FMA) report that summarizes the results of a Computer Crimes Unit (CCU) forensic examination of the reported compromise of an Office of Inspector General (OIG) issued laptop computer.

On September 1, 2010, the Cyber Security Management Center (CSMC) provided OIG with a computer security incident report showing that (b)(5), (b)(7)e

(b)(5), (b)(7)e

Based upon the forensic analysis, it is believed that the (b)(5), (b)(7)e

(b)(5), (b)(7)e

We are forwarding our FMA for informational purposes only. We are closing our file on this matter. If you have any questions, or if we can be of further assistance, please do not hesitate to contact (b)(6), (b)(7)c (work) or (b)(6), (b)(7)c

##

(1) Attachment